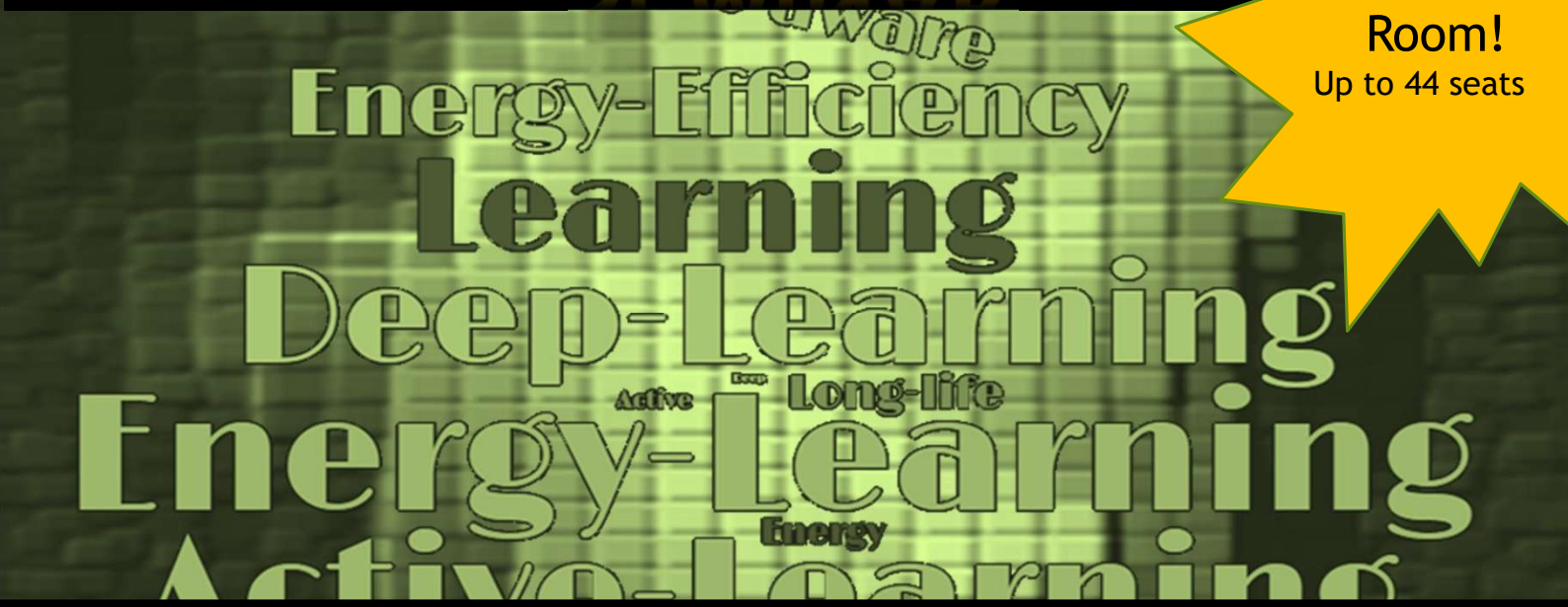
# SEMINAR

New Room!
Up to 44 seats




# Hybrid Deep Learning for Anomaly Detection

## *Description*:

In the field of deep learning, a generative model via an adversarial process gets a great attention due to the amazing demonstration of performance. It can simultaneously train a generative model to capture the data distribution, and discriminative model to estimate the probability that a sample came from the training data. In this talk, I will present a new method of transfer-generative adversarial network (tGAN) with auto-encoders to detect anomaly in malicious software (malware) for computer security. The proposed method of malware detection treats zero-day attacks by generating fake malware and learning to distinguish it from real malware. The data generated from a random distribution are similar but not identical to the real data: it includes modified features compared with real data. The detector learns various malware features using real data and modified data generated by the tGAN based on a deep auto-encoder (DAE), which stabilizes the GAN training. Before training the GAN, the DAE learns malware characteristics, produces general data, and transfers this capacity for stable training of the GAN generator. The trained discriminator passes down the ability to capture malware features to the detector, using transfer learning.

**Funded under projects**
MINECO-TIN2014-56967-R
MINECO-TIN2017-84804-R.

## *Invited Researcher*:

**Prof. Sung-Bae Cho**
Softcomputing Laboratory
Computer Science Dpt.
Yonsei University, Korea

## Short CV:

Dr. Cho received the Ph.D. degree in computer science from KAIST (Korea Advanced Institute of Science and Technology), Korea, in 1993. He was an Invited Researcher of Human Information Processing Research Laboratories at Advanced Telecommunications Research (ATR) Institute, Japan from 1993 to 1995, and a Visiting Scholar at University of New South Wales, Australia in 1998. He was also a Visiting Professor at University of British Columbia, Canada from 2005 to 2006. Since 1995, he has been a Professor in Department of Computer Science, Yonsei University, Korea. Dr. Cho has been serving as an associate editor for several journals including IEEE Transactions on CI and AI on Games (2009-present) and IEEE Transactions on Fuzzy Systems (2013-present). He was also the chair of Games Technical Committee, IEEE CIS (2009-2010), and Student Games-based Competition Subcommittee, IEEE CIS (2011-2012). He is a member of Board of Government (BoG) of Asia Pacific Neural Networks Assembly (APNNA) (2011- present), and a member of three technical committees in IEEE CIS such as Emergent Technologies, Computational Finance and Economics, and Games. His research interests include hybrid intelligent systems, soft computing, evolutionary computation, neural networks, pattern recognition, intelligent man-machine interfaces, and games. He has published over 230 journal papers, and over 680 conference papers.

**Contact info:** villarjose@uniovi.es

**Date:** Tuesday, June the 19th 2018. **Hour:** 12:00 am
**Room: DO-12 Aula Configurable** Sedes Departamentales Oeste, EPI Gijón